AMENDMENTS TO THE CLAIMS

Claims 1-3 (Cancelled)

4. (Previously Presented) A method for enabling an X.509 certificate to support more than one cryptographic algorithm, with an associated public key, comprising the steps of:

providing the X.509 certificate with a signature algorithm with associated public key and signature for all authenticated attributes;

providing the X.509 certificate with a first certificate extension identifying at least one alternative cryptographic algorithm and providing a respective associated public key; and

providing the X.509 certificate with a second certificate extension which contains a signature for each alternative cryptographic algorithm, whereby an alternative cryptographic algorithm may be supported without establishing a new certificate hierarchy.

5. (Previously Presented) The method for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 4, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve and the first and second certificate extensions are identified as non-critical.

6. (Previously Presented) The method for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 4, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

Claims 7-13 (Cancelled)

14. (Previously Presented) The method for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 4, wherein

the signature for all authenticated attributes includes the signing of the second certificate extension, and

the signature for each alternative cryptographic algorithm does not include the signing of the second certificate extension.

Claims 15-16 (Cancelled)